GESTÃO DE RISCOS

Major Fábio de Moura Sousa

O Major de Intendência Moura é aluno do Curso de Pós-Graduação em Gestão de Finanças, Controladoria e Auditoria pela Fundação Getúlio Vargas.

A Gestão de Riscos é um processo conduzido no Exército Brasileiro, que vai desde o Comitê de Governança, Riscos e Controles até o Gestor de Riscos, no estabelecimento de estratégias formuladas para identificar, em toda a Instituição, eventos em potencial capazes de afetá-la e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco estabelecido na Política de Gestão de Riscos do Exército e possibilitar garantia razoável do cumprimento dos seus objetivos.

A fim de viabilizar uma execução simples e eficiente da Gestão de Riscos, iremos abordar uma Metodologia de Gestão de Riscos baseada no referencial presente na obra "Gerenciamento de Riscos Corporativos - Estrutura Integrada" publicada pelo *Committee of Sponsoring Organizations of The Treadway Commission* (COSO), conhecido por COSO ERM, que permitirá aos gestores das Organizações Militares (OM) utilizar uma Matriz de Riscos e Controles (Apêndice A), cujo preenchimento seguirá a ordem de apresentação dos componentes da estrutura de Gestão de Riscos presentes no COSO ERM.

1 GESTÃO DE RISCOS

A definição da Gestão de Riscos reflete certos conceitos fundamentais. A gestão de riscos é:

1. Um processo contínuo e que flui através da organização;
2. Conduzida por militares e civis em todos os níveis da Instituição;
3. Aplicada à definição das estratégias;
4. Formulada para identificar eventos em potencial, cuja ocorrência poderá afetar as Organizações Militares e para administrar os riscos de acordo com o apetite a risco do Exército;

5. Capaz de propiciar garantia razoável quanto o alcance dos objetivos; e

6. Orientada para a realização de objetivos em uma ou mais categorias distintas, porém dependentes.

A Alta Administração do Exército, com base na missão ou visão estabelecida pelo Exército e na Gestão de Riscos coordenada pelo Comitê de Governança, Riscos e Controles, estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da Instituição.

1.1 Estrutura da Gestão de Riscos

Para auxiliar a Alta Administração do Exército no processo de Tomada de Decisão, o Comitê de Governança, Riscos e Controles estrutura a Gestão de Riscos a fim de alcançar os objetivos de controle, classificados em quatro categorias:

1.Estratégico: atingimento das metas gerais, alinhadas com o que suportem à sua missão;

2.Operacional: utilização eficaz e eficiente dos recursos;

3. De Comunicação: confiabilidade de relatórios; e

4. De Conformidade: cumprimento de leis e regulamentos aplicáveis.

O desafio para os Gestores de Risco é reduzir a criticidade do risco em termos de probabilidade e impacto, colocando-o num nível aceitável. Após a avaliação dos riscos, inicia-se a avaliação do nível de riscos do processo

Quando se constata que a Gestão de Riscos é eficaz em cada uma das quatro categorias de objetivos, isso significa que o Comandante do Exército e a Alta Administração terão garantia razoável de que entenderam até que ponto os objetivos estratégicos e operacionais estão realmente sendo alcançados, o sistema de comunicação da Instituição é confiável e todas as leis e regulamentos cabíveis estão sendo observados.

A Gestão de Riscos está estruturada em oito componentes inter-relacionados e integrados com o processo de gestão das Organizações Militares. Esses componentes são:

1. Ambiente interno: inclui, entre outros elementos, integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança organizacional, políticas e práticas de recursos humanos. O ambiente interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos;

2. Fixação de objetivos: todos os níveis do Exército Brasileiro (Alta Administração, Departamentos, Diretorias e Organizações Militares) devem ter objetivos fixados e comunicados. A explicitação de objetivos, alinhados à missão e à visão da organização, é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução;

3. Identificação de eventos: devem ser identificados e relacionados os riscos inerentes à própria atividade da organização, em seus diversos níveis;

4. Avaliação de riscos: os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos deve ser feita por meio de análises qualitativas, fazendo uso de lógica intuitiva com critérios preestabelecidos e escala de valoração para determinar o nível do risco. Os riscos devem ser avaliados quanto à sua condição de inerentes ou residuais;

5. Resposta a riscos: a Organização Militar deve identificar qual estratégia seguir (evitar, mitigar, compartilhar ou aceitar) em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de exposição aos riscos previamente estabelecidos pelo Exército Brasileiro em confronto com a avaliação que se fez do risco;

6. Atividades de controles internos: são as políticas e os procedimentos estabelecidos e executados para mitigar os riscos que a organização tenha optado por tratar. Também denominadas de procedimentos de controle, devem estar

distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão preventivos e detectivos, bem como a preparação prévia de planos de contingência e resposta à materialização dos riscos;

7. Informação e comunicação: informações relevantes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, como também com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam a informação fluir em todos os sentidos; e

8. Monitoramento: tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos.

2 PROCESSO DE GESTÃO DE RISCOS

Os gestores das Organizações Militares poderão executar a Gestão de Riscos de maneira simples e eficiente, utilizando a Matriz de Riscos e Controles (Apêndice), cujo preenchimento seguirá a ordem de apresentação dos seguintes componentes da estrutura de Gestão de Riscos presentes no COSO ERM:

1. Fixação de Objetivos

A fixação de objetivos é uma precondição à identificação de eventos, à avaliação de riscos e às respostas a riscos. É necessário que os objetivos existam para que a Organização Militar possa identificar e avaliar os riscos quanto a sua realização, bem como adotar as medidas necessárias para administrá-los.

Como os processos dão suporte a execução das estratégias definidas pelos gestores para o atingimento dos objetivos estratégicos da Organização Militar, a Gestão de Riscos será executada por processo. Por qual processo o gestor deve iniciar a Gestão de Riscos? Deve iniciar pelos processos mais críticos da OM.

Após a priorização dos processos mais críticos a serem analisados, devem-se definir os objetivos do processo em análise e lançá-los na Matriz de Riscos e Controles (Apêndice).

2. Identificação de Eventos

Neste componente, a OM identifica os eventos em potencial que, se ocorrerem, afetarão a organização, por possuírem efeitos adversos na sua capacidade de implementar adequadamente a estratégia e alcançar os objetivos. Estes eventos representam riscos que exigem avaliação e resposta da OM. A Figura 1 apresenta uma visão ampla sobre os conceitos de risco, evento, causa, consequência, probabilidade e impacto.

3. Avaliação de Riscos

Uma infinidade de causas internas e externas (fatores de risco) impulsiona os riscos que afetam a implementação da estratégia e o cumprimento dos objetivos. Como parte da gestão de riscos, a OM

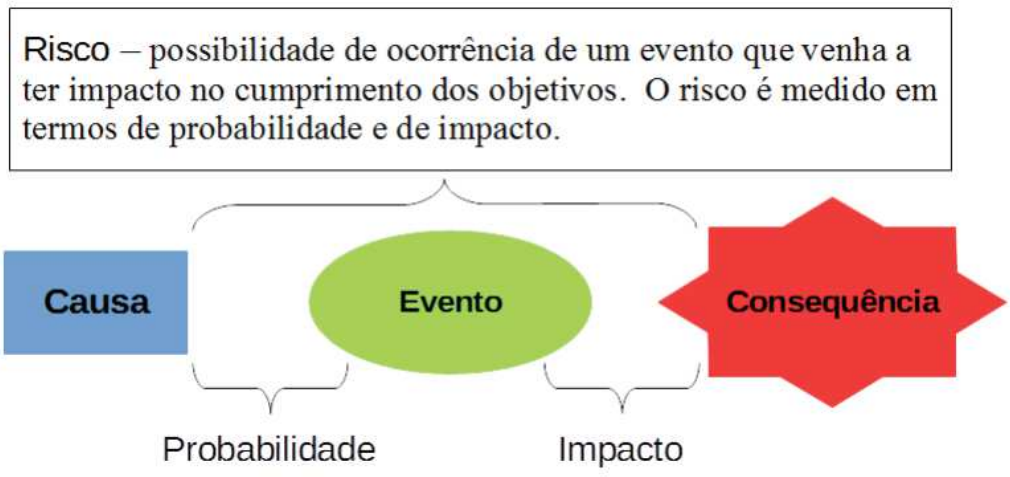

Figura 1: Esquema do Risco
Fonte: Elaborado pelo autor

deve reconhecer a importância de compreender essas causas e o risco que pode emanar delas.

A OM pode optar pela técnica do Diagrama de Causa e Efeito, chamada Diagrama de Ishikawa, para poder entender quais são os fatores de risco que influenciam a concretização de cada risco.

Os fatores de risco são compostos pela vulnerabilidade existente em uma determinada Fonte de Risco.

A Fonte de Risco é um elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco:

- Pessoas - que podem não estar capacitadas, vir a cometer erro não-intencional ou fraude;
- Processos - que podem apresentar problemas de modelagem, transação, conformidade, controle ou técnica apropriada;
- Sistemas de gestão - que podem apresentar problemas de padronização e de inter-relacionamento com outras atividades;
- Infraestruturas física e organizacional – que podem ser departamentalizadas ou descentralizadas;
- Tecnologia de produto ou de produção - equipamentos; sistemas informatizados e confiabilidade da informação; e
- Eventos externos - que não são gerenciáveis.

A OM poderá utilizar a técnica de Análise de Fluxo de Processo, que reúne as entradas, as tarefas, as responsabilidades e as saídas que se combinam para formar um processo. Devem ser considerados os fatores de risco internos e externos locando-os com bandeirolas vermelhas, que afetam as entradas ou as atividades em um processo, ao se identificar os riscos, também locados com bandeirolas vermelhas, que podem afetar o cumprimento dos objetivos deste processo. A utilização desta técnica permite que o Gestor de Riscos saiba em que tarefas específicas do processo os fatores de riscos influenciam na concretização dos riscos, bem como, o momento em que os riscos se manifestam. Este conhecimento será de suma importância para a eficácia dos controles internos da gestão que serão implementados para dar resposta aos riscos.

Entende-se por riscos inerentes a avaliação dos riscos sem considerar a execução de controles para mitigá-los. Dentro desse conceito é necessário elaborar a avaliação de riscos inerentes (probabilidade x impacto), cujo resultado será o grau de criticidade do risco (magnitude) consolidado na Matriz de Riscos e Controles.

A avaliação de riscos visa auxiliar na definição de prioridades e opções de tratamento aos riscos identificados. A metodologia a ser utilizada pela OM para a avaliação de riscos possui dois parâmetros claros a serem estudados:

Descritor	Descrição	Nível
Muito alta	Evento se reproduz muitas vezes, se repete seguidamente, de maneira assídua, numerosa e, não raro, de modo acelerado. Interfere de modo claro no ritmo das atividades, sendo evidente para os que conhecem o processo.	5
Alta	Evento usual, corriqueiro. Devido à sua ocorrência habitual ou conhecida em uma dezena ou mais de casos, aproximadamente, seu histórico é amplamente conhecido por parte de gestores e operadores do processo.	4
Média	Evento esperado, que se reproduz com frequência reduzida, porém constante. Seu histórico de ocorrência é de conhecimento da maioria dos gestores e operadores do processo.	3
Baixa	Evento casual, inesperado. Muito embora raro, há histórico conhecido de sua de ocorrência por parte dos principais gestores e operadores do processo.	2
Muito baixa	Evento extraordinário para os padrões conhecidos da gestão e operação do processo. Embora possa assumir dimensão estratégica para a manutenção do processo, não há histórico disponível de sua ocorrência.	1

Tabela 1: Avaliação qualitativa da Probabilidade
Fonte: Elaborado pelo autor

• Saber qual a chance, a probabilidade, dos riscos virem a acontecer, frente à condição existente de cada processo e área de negócio; e

• Calcular o impacto, as consequências para o processo impactado.

O impacto sobre os objetivos de um processo poderá acontecer em uma ou mais dimensões, tais como: prazo, orçamentário-financeiro, qualidade, escopo, imagem ou reputação, etc.

Para determinar os níveis de risco, é preciso definir escalas para estimar a probabilidade e o impacto, bem como estabelecer quando a combinação desses dois fatores representa um risco baixo, médio, alto, etc.

As Tabelas 1 e 2 exemplificam as escalas qualitativas que auxiliam na estimativa de probabilidades e impactos de eventos.

Com o objetivo de visualizar e, ao mesmo tempo, implementar uma forma de tratamento de cada risco, o resultado da avaliação dos riscos será apresentado em um mapa de riscos, chamado de Diagrama de Verificação de Riscos (DVR) permitindo o acompanhamento da mitigação ou elevação dos riscos.

O Diagrama de Verificação de Riscos (Figura 2) demonstra os pontos de cruzamento da probabilidade de ocorrência e do impacto dos riscos. Desta forma, pela divisão do diagrama em quadrantes, pode-se avaliar a criticidade dos riscos. Quanto maior for a probabilidade e o impacto de um risco, maior será seu nível de criticidade.

Quanto à criticidade, os riscos possuem as seguintes características:

• Risco no quadrante vermelho: risco inaceitável, que possui alta probabilidade de ocorrência e poderá resultar em impacto extremamente severo; caso ocorra, exige tratamento imediato, colocando-se em execução um plano de ação composto por controle preventivo, para eliminar suas causas ou reduzir sua frequência; controle detectível e plano de contingência para reduzir sua severidade;

• Risco no quadrante laranja: pode ser tanto um risco provável, que possui alta probabilidade de ocorrência e baixo impacto na consecução dos objetivos; bem como um risco inesperado, que possui baixa probabilidade de ocorrência e alto impacto na consecução dos objetivos. A estas ameaças, deve-se possuir respostas rápidas ao serem detectadas, portanto, devem estar planejadas e testadas em um plano de contingência, emergência, continuidade de negócios, além de ações preventivas. Diferem-se dos riscos do quadrante vermelho, por terem ações de tratamento implementadas com mais planejamento e tempo. São eventos que devem ser constantemente monitorados;

Descritor	Descrição	Nível
Muito alto	Interrupção abrupta de operações, atividades, projetos, programas ou processos da organização, impactando fortemente outros processos, causando impactos de dificílima reversão nos objetivos.	5
Alto	Interrupção de operações, atividades, projetos, programas ou processos da organização, causando impactos de reversão muito difícil nos objetivos.	4
Médio	Interrupção de operações ou atividades da organização, de projetos, programas ou processos, causando impactos significativos nos objetivos, porém recuperáveis.	3
Baixo	Degradação de operações, atividades, projetos, programas ou processos da organização, causando impactos pequenos nos objetivos.	2
Muito baixo	Degradação de operações, atividades, projetos, programas ou processos da organização, porém causando impactos mínimos nos objetivos (de tempo, prazo, custo, quantidade, qualidade, acesso, escopo, imagem, etc.) relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários).	1

Tabela 2: Avaliação qualitativa do Impacto
Fonte: Elaborado pelo autor

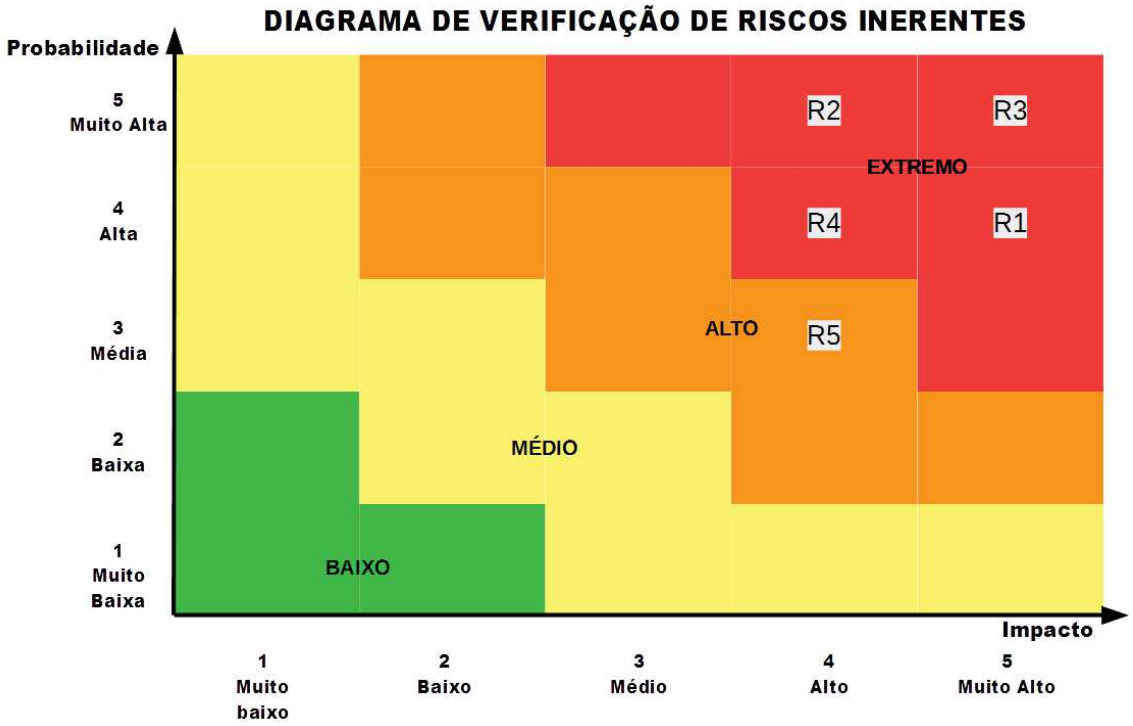

Figura 2: Diagrama de Verificação de Riscos Inerentes
Fonte: Elaborado pelo autor

- Risco no quadrante amarelo: risco que deve ser quantificado e monitorado de forma rotineira e sistemática, porque suas consequências são gerenciáveis, podendo também possuir planos de contingência; e
- Risco no quadrante verde: risco que representa pequeno problema e causa pouco prejuízo, portanto controlável.

O desafio para os Gestores de Risco é reduzir a criticidade do risco em termos de probabilidade e impacto, colocando-o num nível aceitável.

Após a finalização da etapa de avaliação dos riscos, inicia-se o processo de avaliação do nível de riscos do processo.

O Nível de Risco é um índice que deve ser calculado sempre que houver a avaliação de riscos, possibilitando mensurar o nível de criticidade dos processos analisados, visando facilitar o monitoramento e acompanhamento da evolução dos riscos. O índice é calculado pela multiplicação da média dos graus de probabilidade com a média dos graus de impacto dos riscos presentes nos processos, projetos, áreas ou organizações.

O Nível de Risco pode ser classificado em:

- Extremo – processos que tem alto grau de risco e poderão resultar em impacto extremamente severo. Exigem implantação imediata das estratégias de prevenção e proteção, ou seja, ação imediata;
- Alto – processos que devem receber tratamento em médio ou curto prazo. Possuem baixo grau de risco e elevados impactos. São processos que devem ser constantemente monitorados;
- Médio – processos com alto grau de risco, mas que causam consequências gerenciáveis à organização. Esses processos devem ser monitorados de forma rotineira ou sistemática; e
- Baixo – processos que estão na zona de conforto, devendo ser gerenciados.

4 Resposta a Riscos

Após a finalização do processo relativo ao componente de Avaliação de Riscos, é iniciado o processo do componente Respostas a Riscos.

A OM deve identificar qual estratégia seguir (aceitar, compartilhar, evitar ou mitigar) em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco.

A priorização deve estar embasada no Diagrama de Verificação de Riscos. O risco no quadrante vermelho deve receber prioridade no tratamento.

5 Atividades de Controle

Atividades de controles internos são estabelecidas e executadas quando a OM tenha optado pela estratégia da mitigação no componente

Respostas a risco.

Incluem uma gama de Controles Internos da Gestão preventivos e detectivos, bem como a preparação prévia de Planos de Contingência e resposta à materialização dos riscos.

São exemplos de Controles Internos da Gestão: alçadas, autorizações, conciliações, revisões de desempenho, segurança física, segregação de função, normas, procedimentos e sistemas informatizados.

A fim de possibilitar ao gestor a definição dos controles a serem implementados visando a mitigação dos riscos do processo, faz-se necessário alinhar os controles aos fatores de riscos e aos riscos.

O entendimento sobre o fluxo das atividades do processo e desenho dos controles, classificados como preventivos e detectivos permite avaliar se o dimensionamento destes controles atendem ou não ao objetivo esperado.

Para auxiliar esta avaliação e incluir os controles e planos de contingência na Matriz de Riscos e Controles, utiliza-se as seguintes informações:

- Controle: é uma ação tomada para certificar-se de que algo se cumpra. Os controles também são meios usados para verificar que certa ação é eficiente ao seu propósito. Exemplo: conferência de entradas manuais de dados no sistema;
- Tipo de controle: manual ou automático (sem intervenção humana);
- Objetivo do controle: atingimento das metas; utilização eficiente e eficaz dos recursos; confiabilidade das informações e cumprimento normativos aplicáveis. Exemplo: garantir que toda e qualquer informação inserida no sistema seja íntegra e completa;
- Periodicidade do uso do controle: diário, quinzenal, mensal, etc; e
- Categoria do controle:

1. Preventivo – desenhado para prevenir eventos indesejáveis. Reduz a probabilidade dos fatores de risco virem a contribuir para a concretização dos riscos; e

2. Detectivo – desenhado para detectar eventos indesejados. Detecta a manifestação/ocorrência de um risco, sendo necessário um plano de contingência para mitigar o impacto nos objetivos do processo.

A Figura 3 apresenta a localização dos controles preventivos, controles detectivos e planos de contingência em relação à causa, ao evento e às consequências.

A fim de garantir que os possíveis riscos (alinhados a cada objetivo do processo) foram identificados, analisados e avaliados e que os controles preventivos (necessários para mitigar a probabilidade dos fatores de risco virem a contribuir para a concretização dos riscos) e os planos de contingência (associados a controles detectivos para mitigar o impacto nos objetivos do processo) foram elaborados e implementados, faz-se necessário realizar uma análise na Matriz de Riscos e Controles (Apêndice).

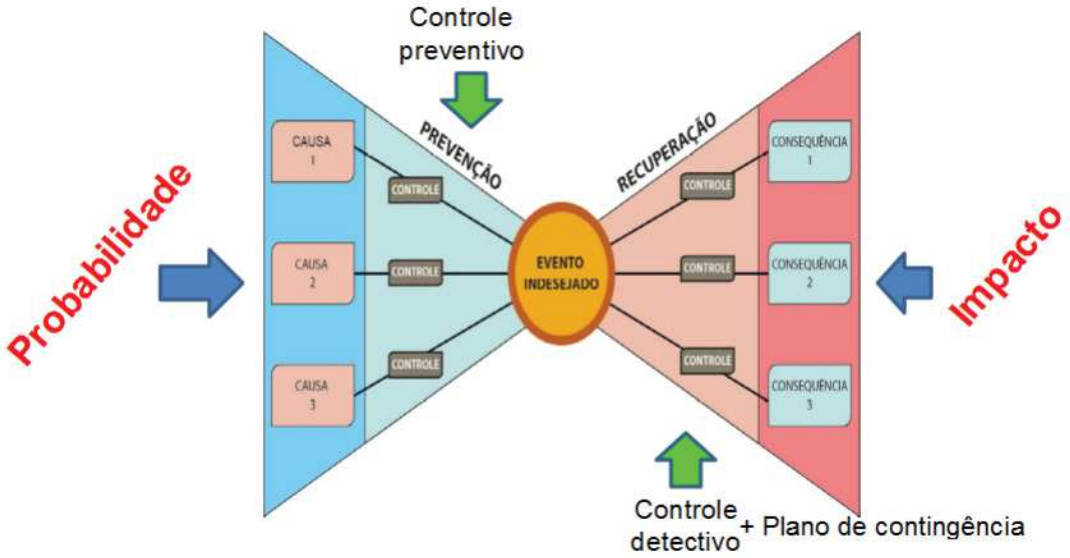

Figura 3: Controles Preventivos e Detectivos (Técnica Bow-Tie)
Fonte: Elaborado pelo autor

Os itens abaixo são alguns exemplos de conclusão da análise na Matriz de Riscos e Controles:

- O risco 'R1' foi avaliado como extremo (25 pontos). Entretanto, não há controle preventivo para mitigar a alta probabilidade do fator de risco 'FR 1' em contribuir para a concretização do risco R1; bem como, não há um plano de contingência associado ao controle detectivo 'C5' que possa dar início a mitigação do impacto muito alto de se gerar desperdício de recursos públicos, quando da constatação da ocorrência do risco pelo controle C5;
- A estratégia de tratamento escolhida para responder ao o risco 'R4' foi equivocada, pois não se pode aceitar um risco extremo; e
- Todo objetivo incorre, pelo menos, em um risco. Portanto, verifica-se que não foi identificado nenhum risco para o objetivo 'O5'.

O resultado desta análise resultará em recomendações de melhorias na Gestão de Riscos, as quais poderão ser implementadas por meio de Planos de Ação.

A seguir, estão listados algumas recomendações de melhorias na Gestão de Riscos:

- Elaborar e implementar um controle preventivo e um plano de contingência associado ao controle detectivo para mitigar o risco R1;
- Selecionar outra estratégia para dar uma resposta ao risco R4; e
- Identificar e avaliar os riscos que poderão impactar o objetivo O5.

Após a execução dos Planos de Ação que permitiram a implementação de melhorias na Gestão de Riscos, faz-se necessário reavaliar os riscos a fim de recalcular a probabilidade e o impacto dos riscos inerentes, sob a ótica de que controles internos foram implementados a fim de mitigá-los.

Neste momento, os riscos passam a ser considerados como riscos residuais estimados. Ou seja, após a implementação de controles internos e reavaliação dos riscos, o gestor estima um novo grau de criticidade para os riscos, bem como para o processo.

6 Atividades de Controle

O monitoramento deve ser planejado como parte do processo e deve envolver a checagem ou vigilância regulares. Pode ser periódico ou acontecer em resposta a um fato específico.

De forma clara e objetiva o monitoramento envolve três procedimentos:

- O primeiro procedimento é verificar se o Plano de Ação proposto foi executado. Para isso, devemos utilizar os indicadores: Executado, Em Execução e Não Executado. Também devem ser acompanhados os resultados das ações e medidas propostas. Devem ser acompanhadas para saber se seus objetivos foram atingidos e, se não foram, quais as dificuldades encontradas e as ações corretivas;
- O segundo procedimento é acompanhar a evolução das condições dos riscos identificados e analisados. Neste caso, deve-se verificar se as condições listadas no diagrama de causa e efeito sofreram mudanças e/ou alterações do ambiente, e
- O terceiro procedimento tem como objetivo possibilitar ao gestor o conhecimento do processo, no que tange à eficácia, ineficácia ou inexistência dos controles para que seja realizada uma análise dos riscos residuais estimados.

A OM deve identificar qual estratégia seguir (aceitar, compartilhar, evitar ou mitigar) em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de exposição a riscos estabelecido em confronto com a avaliação realizada.

Esse entendimento sobre o fluxo das atividades e desenho dos controles, classificados como preventivos ou detectivos, permite avaliar se o dimensionamento destes controles atendem ou não o objetivo esperado.

O resultado é a verificação da eficácia do controle, medida em porcentagem de vezes que o controle mitigou o risco. Exemplo: Para um determinado processo, foi implementado um controle interno visando mitigar a probabilidade

de manifestação de um risco (controle preventivo). Ao realizar a avaliação da eficácia do controle, foi verificado que de cada 10 vezes que o processo foi executado, o controle preveniu que o risco se manifestasse em três vezes, ou seja, o controle foi eficaz em apenas 30%.

O parecer é a descrição da eficácia do controle, comparando o resultado da avaliaço da eficácia do controle com o critério estabelecido. Exemplo: Foi estabelecido que o critério de eficácia para que os controles sejam considerados eficazes é de 90%. Desta forma, de cada 10 vezes que o processo for executado, o controle deverá preveni que o risco se manifeste em, no mínimo, nove vezes. Portanto, o controle com resultado de 30% obterá o parecer de 'ineficaz'.

Após o monitoramento do controle, faz-se necessário reavaliar os riscos, ou seja, recalcular a probabilidade e o impacto dos riscos residuais estimados. As notas de probabilidade e impacto devem ser revistas neste momento, de forma coerente com a avaliação realizada sobre os controles.

Neste momento, os riscos passam a ser considerados como riscos residuais efetivos. Ou seja, após a execução do monitoramento e da reavaliação dos riscos, o gestor passa a verificar o real grau de criticidade dos riscos, bem como do processo. Este processo de monitoramento é de suma importância e deve ser acompanhado diretamente pelo gestor de riscos.

CONSIDERAÇÕES FINAIS

Apresentamos nesta publicação metodologia, critérios e técnicas para a execução do Processo de Gestão de Riscos numa organização, independente de seu porte ou autonomia administrativa.

A metodologia apresentada foi formulada com base no referencial presente na obra "Gerenciamento de Riscos Corporativos – Estrutura Integrada" publicada pelo *Committee of Sponsoring Organizations of The Treadway Commission* (COSO).

Nesta metodologia, dividimos a Estrutura da Gestão de Riscos em oito componentes inter-relacionados e integrados com o processo de gestão das Organizações Militares, a saber: Ambiente Interno, Fixação de Objetivos, Identificação de Eventos, Avaliação de Riscos, Resposta a Riscos, Atividades de Controles Internos, Informação e Comunicação, além do Monitoramento.

A Alta Administração da organização deve valer-se do Planejamento Estratégico e/ou Plano de Gestão para fixar os objetivos do processo, cuja Gestão de Riscos será executada, alinhando-os aos objetivos estratégicos da sua organização. Esse alinhamento é imprescindível para que os processos que dão suporte a organização, possam efetivamente contribuir para o atingimento das metas e objetivos traçados no seu planejamento estratégico.

Cabe ressaltar que cada objetivo do processo incorre em pelo menos um risco. Entretanto, cada risco pode ser concretizado/manifestado pela influência de um ou mais fatores de risco (causas), bem como gerar uma ou mais consequências nos objetivos do processo. Portanto, recomenda-se a utilização da Técnica *Bow-Tie* (gravata borboleta) para realizar a análise do risco.

Os riscos sofrem evolução ao longo do Processo de Gestão de Riscos, a medida que são analisados. Na primeira análise, isenta de qualquer ação de controle, são considerados riscos inerentes.

Após o estudo da melhor estratégia de tratamento para dar uma resposta ao risco, desenha-se controles preventivos, controles detectivos e planos de ação, quando a estratégia escolhida for a mitigação do risco. Neste momento, vislumbra-se um novo grau de criticidade do risco, passando a chamar-se de risco residual estimado.

Contudo, no Processo de Gestão de Riscos, faz-se necessário monitorar a implementação dos diversos planos de ação propostos, nos quais incluem-se a elaboração, aperfeiçoamento e implementação dos controles internos e dos planos de contingência. Dessa forma, o gestor reavalia os riscos, com base nas ações de monitoramento, auferindo um grau de criticidade mais próximo da realizada. Nesse ponto, o risco passa a ser denominado de risco residual efetivo.

Diante da conclusão da execução das oito etapas do Processo de Gestão de Riscos, o gestor possuirá informações mais precisas para a tomada de decisão.

Portanto, verifica-se a importância para o gestor integrar a Gestão de Riscos em todos os níveis da Gestão dos Processos Organizacionais, bem como da Gestão de Projetos.

APÊNDICE – MATRIZ DE RISCOS E CONTROLES

Processo:																																	
Fixação de Objetivos		Identificação de Eventos		Avaliação de Riscos								Resposta a Risco	Atividade de Controle									Monitoramento											
Objetivos do processo	Nº O	Riscos inerentes aos objetivos	Nº R	Fator de Risco (Causa)		Nº FR	Consequência	Avaliação de risco inerente				Estratégia de Tratamento dos Riscos	Controles preventivos	Nº C	Controles detectivos	Nº C	Planos de contingência	Nº P	Avaliação de risco residual estimado				Controles preventivos		Controles detectivos e Planos de Contigência		Avaliação de risco residual efetivo					
				Fonte	Vulnerabilidade			P	I	P x I	Magnitude								P	I	P x I	Magnitude	Avaliação	Eficácia >90%	Avaliação	Eficácia >90%	P	I	P x I	Magnitude		
Solicitar ...	O1	Não atendimento de ...	R1	Processos	Ausência de ...	FR 1	Desperdício de recursos públicos	4	5	20	Extremo	Mitigar	Alta Administração pública normativo criando obrigatoriedade de ...	C1	Assessoria Jurídica verifica ...	C5	Assessoria jurídica não aprova ...	P5	2	2	4	Médio	90%	Eficaz	70%	Ineficaz	2	5	10	Alto		
Realizar ...	O2	Contratação com ...	R2	Processos	Ausência de ...	FR 2	Superfaturamento	5	4	20	Extremo	Mitigar	Realização de ...	C2	Fiscal Administrativo verifica ...	C6	Fiscal Administrativo devolve ...	P6	2	2	4	Médio	50%	Ineficaz	30%	Ineficaz	5	4	20	Extremo		
Descrever ...	O3	Contratação com ...	R3	Processos	Descrição inadequada do ...	FR 3	Comprometimento da qualidade das atividades	5	5	25	Extremo	Mitigar	Elaboração de ...	C3	Fiscal Administrativo verifica ...	C7	Fiscal Administrativo devolve ...	P7	2	3	6	Médio	95%	Eficaz	90%	Eficaz	2	3	6	Médio		
						Nível de Risco do Processo				18,6	Extremo						Nível de Risco do Processo				3,8	Médio		Nível de Risco do Processo					8,6	Alto		

REFERÊNCIAS

BRASIL. Ministério da Defesa. Comando do Exército. Portaria nº 813-Cmt Ex, de 28 de setembro de 2012: aprova as Normas para a Realização das Atividades de Auditoria e Fiscalização pelo Controle Interno do Comando do Exército (EB10-N-13.003). Boletim do Exército. Brasília, DF, 2012.

_____. Ministério da Defesa. Comando do Exército. Portaria nº 018-Cmt Ex, de 17 de janeiro de 2013: aprova o Manual de Auditoria (EB 10-MT-13.001) e dá outras providências. Boletim do Exército. Brasília, DF, 2013.

_____. Ministério da Defesa. Comando do Exército. Portaria nº 465-Cmt Ex, de 17 de maio de 2017: aprova a Política de Gestão de Riscos do Exército Brasileiro (EB 10-P-01.004), Boletim do Exército. Brasília, DF, 2017.

_____. Ministério da Defesa. Comando do Exército. Portaria nº 222-EME, de 5 de junho de 2017: aprova a Metodologia da Política de Gestão de Riscos do Exército Brasileiro (EB 20-D-07.089), Boletim do Exército. Brasília, DF, 2017.

_____. Tribunal de Contas da União. Revista do Tribunal de Contas da União número 132, janeiro/abril 2015. Metodologia de Auditoria com Foco em Processo e Risco. Brasília: TCU, 2015. p. 28. Disponível em: <http://portal.tcu.gov.br/publicacoes-institucionais/periodicos-e-series/revista-do-tcu/>.

BRASILIANO, Antônio Celso Ribeiro. GESTÃO DE RISCO DE FRAUDE: Fraud Risk Assessment - FRA. Sicurezza Editora, 2015.

COSO. Committee of Sponsoring Organizations of the Treadway Commission. Gerenciamento de riscos corporativos. Tradução Audibra e PricewaterhouseCopers. São Paulo: [s.n.], 2013, 135 p.

DE CICCO, Francesco. AUDITORIA BASEADA EM RISCOS: Como implementar a ABR nas organizações: uma abordagem inovadora. Risk Tecnologia Editora Ltda, 2007.